Voice Over Internet Protocol (VOIP) SECURITY

Rick Kuhn
Computer Security Division
National Institute of Standards and Technology

Major VOIP Issues

- **Much lower cost**
  - PC + headset + software = telephone
  - VOIP service cheaper too
- **Quality of service** – less than POTS,but that doesn't matter (see above)
- **Much less secure** against *low-end* attackers
  - Hacker's paradise
  - Script kiddies and petty criminals
  - VOIP + touch-tone menus = big fraud opportunities!
  - Much easier on-hook audio, traffic analysis

Telecom Convergence

- **National Security Emergency Preparedness Communications Convergence Policy Review**

"Convergence implies new vulnerabilities as well as opportunities for NS/EP. Though communication capabilities will expand, the Intelligence Community assesses that convergence is the technological trend most likely to aid those who want to attack communications compared to those responsible for defense."

Firewalls and QoS

- Problem: Firewall traffic investigation adds latency to the system and heavy data traffic can introduce jitter.
- Solutions:
  - Implement firewalls with fast CPU’s to handle the high rate of packet delivery.
  - Use QoS aware firewalls

IPSec and QoS

- Problem: Encryption also introduces latency / jitter
  - Encryption/decryption process takes time
  - Crypto-engine schedulers do not implement QoS
- Solutions:
  - Packet compression schemes have experimentally aided performance
  - QoS-aware scheduling before and after encryption heuristically improves performance.

Disrupting Call Setup

- Problem:
  - Firewalls can block the call setup ports and NAT can change the IP address/ports being used internally.
- Solutions:
  - Incorporate an ALG or FCP into the architecture that can manipulate the setup packets' data.

What Should You Do Now? Network tools

- Separate voice and data traffic using separate address space, virtual LANs as much as possible
  - Reduce risk of data sniffers
  - Can tune IDSs for voice and data separately
- *Use firewalls designed for VOIP traffic*
- *At the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or MGCP connections from the data network*

What Should You Do Now? Protecting voice data

- Avoid PC-based “softphones” if practical
  - Keeps voice and data separate
- Use access control, encryption, where possible
- *Use IPSec or SSH for all remote management and auditing access*
- *Don't forget to plan for E911, emergency backup, other special considerations*

Future Prospects for VOIP Security

- Cost considerations dominate
- More home users
  - Will remain vulnerable
  - How long before VOIP-backdoor worm? (e.g., to sniff credit-card numbers)
- Corporate users
  - Improved recognition of security issues
  - Modest improvement in security (not unlike corporate PC security)

Summary

- VOIP security requires adapting traditional network security measures for a high speed, dynamic environment.
- For more info see:

  “Security Considerations for Voice Over IP Systems”
  NIST SP 800-58 D. Richard Kuhn, Thomas J. Walsh, Steffan Fries
  http://csrc.nist.gov/publications/drafts.html